IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. MAKSIM BEREZAN, *Defendant.*	No. 1:20-cr-145 The Honorable T.S. Ellis, III

STATEMENT OF FACTS

The United States and the defendant, MAKSIM BEREZAN, agree that the following facts are true and correct, and that, had this matter proceeded to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence.

1. From at least in or around July 2009, through at least in or around December 2015, BEREZAN knowingly and unlawfully conspired with other persons known and unknown to commit a variety of offenses, including:

a. Devising and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, such scheme affecting a financial institution, and for the purposes of executing such scheme and artifice transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, and signals, in violation of Title 18, U.S. Code, Sections 1343 and 1349, as charged in Count One of the Indictment.

b. Knowingly and with intent to defraud, trafficking in and using one or more unauthorized access devices during a one-year period, and by such conduct obtaining

things of value aggregating $1,000 or more during that period, in violation of Title 18, U.S. Code, Sections 371 and 1029(a)(2), as charged in Count Five of the Indictment; and

c. Intentionally accessing a computer without authorization and exceeding authorized access, and thereby obtaining information from a protected computer in which such access was for purposes of private financial gain, in violation of Title 18, U.S. Code, Sections 371, 1030(a)(2)(C), and 1030(c)(2)(B), as charged in Count Five of the Indictment.

2. The conspiracies into which BEREZAN entered and furthered arose from his membership in DirectConnection, an exclusive website that provided a secure space through which individuals engaging in computer crimes could meet and assist each other in planning and carrying out a variety of malicious and fraudulent cyber activities.

3. DirectConnection was launched on or about February 21, 2009. The website was accessible worldwide, including from the Eastern District of Virginia, via an internet connection.

4. BEREZAN joined DirectConnection on or about July 15, 2009. Thereafter, and continuing through at least in or around December 2015, BEREZAN and other DirectConnection members used the relationships they developed on DirectConnection to further the criminal aims of DirectConnection itself and to devise other criminal ventures, which they sometimes furthered outside the auspices of DirectConnection. For example:[1]

a. On or about August 8, 2011, while in the United States, a DirectConnection co-conspirator posted a message within the "Sale and purchase of cards. Visa, MasterCard, AMEX. COBs, VBV, CVV. Extraction of SSN/DOB and other cardholder information" forum that included his email address and stated: "We're selling US CC with a

[1] All postings or messages on DirectConnection or communications by co-conspirators referenced in this Statement of Facts are translations from Russian to English.

known available balance. 100% validity. It's possible to pick by the state. Prices: $5 for a CC + $0.5 for every 1K on the balance (that is 1-2K available balance = $5.5, 2-3K = $6.5 etc)."

b. Likewise, on or about November 12, 2011, Co-Conspirator-1 posted an advertisement on DirectConnection for a website selling stolen payment card data, including data belonging to residents in the Eastern District of Virginia and cards that had been issued by Financial Institution A, a U.S. banking entity headquartered in Virginia, within the Eastern District of Virginia, and then insured by the Federal Deposit Insurance Corporation (FDIC).

c. Moreover, on or about October 4, 2015, a DirectConnection co-conspirator posted an advertisement indicating that he wished to sell a database containing the names and dates of birth of millions of Americans. This database contained the personal information of American citizens residing in the Eastern District of Virginia.

5. BEREZAN was an active user of DirectConnection. BEREZAN furthered the operation of DirectConnection and its criminal aims in a variety of ways, such as by vouching for users, paying fees, participating in a dispute resolution mechanism, alerting other DirectConnection users of law enforcement activity, and communicating with other DirectConnection users about certain unlawful services. For example:

a. On or about September 29, 2010, BEREZAN utilized DirectConnection's dispute resolution mechanism. BEREZAN, in particular, made a "claim" against another DirectConnection user, alleging that the user had "falsely accused [BEREZAN] of scamming without providing any proof," and asked the DirectConnection "administrators to address this situation" by requiring the other DirectConnection user to produce "proofs" or implementing a "ban on this site" of that user.

b. Similarly, on or about October 6, 2010, BEREZAN posted a message within the "General section. Skirmishes, complaints, debtors and exposure of scammers" forum of Direct Connection that accused another DirectConnection user of borrowing money from BEREZAN and failing to pay it back. BEREZAN warned that the other DirectConnection user had "played a dirty trick," asked "the administrators to take measures," and demanded his money back plus "double for such a dirty trick."

c. Likewise, on or about October 11, 2012, BEREZAN filed a complaint on DirectConnection against another user for referring BEREZAN to an individual who used stolen payment card data provided by BEREZAN to withdraw cash but did not remit any of the proceeds from the fraudulent withdrawals to BEREZAN.

d. BEREZAN also vouched for other users. On or about June 12, 2014, BEREZAN sent a private message to "Support" for DirectConnection indicating that BEREZAN was "vouching" for a particular user. This user had asked BEREZAN to vouch for him.

e. In addition, BEREZAN paid membership fees to DirectConnection as indicated by a private message that BEREZAN sent on or about August 10, 2014, to "Support" for DirectConnection. BEREZAN wrote in this message that he was having difficulty paying a "forum fee" of $105 for three months' worth of access to the website.

f. BEREZAN also flagged articles that might be of interest to DirectConnection members. On or about September 24, 2012, BEREZAN posted a message within the "Media. News, publications, journalist articles and everything related to our subject" forum on DirectConnection regarding Thailand law enforcement's arrest of two Russians for using stolen bank data to engage in unauthorized withdrawals. And, on or about December 1, 2014, BEREZAN posted a message within the "Media. News, publications, journalist articles

and everything related to our subject" forum on DirectConnection with a link to a security researcher's online posting about malware being used to hack ATMs. BEREZAN requested that anyone "related to that" (*i.e.*, the hack of ATMs with malware) to contact BEREZAN.

6. BEREZAN also used DirectConnection as a means to connect with other cybercriminals interested in acquiring and using stolen payment card information. For example:

a. On or about August 25, 2010, BEREZAN posted a message within the "Cyber security. Programming. Cracking. Cracking, data bases, bot nets. Trojans and scripts. Exploits" forum on DirectConnection in which he requested access to a botnet—*i.e.*, a network of compromised internet-connected devices—in the United States. BEREZAN offered to provide the "injects"—that is, malicious code that targets web browsers—designed to steal payment card numbers, card verification values (CVVs), expiration dates, and PINs,[2] and would share the proceeds derived from "cashouts."[3]

b. Then, on or about November 25, 2010, BEREZAN posted a message within the "Cyber security. Programming. Cracking. Cracking, data bases, bot nets. Trojans and scripts. Exploits" forum on DirectConnection asking for assistance in extracting payment card information from wireless networks in grocery stores and decrypting PINs.

c. On or about December 8, 2010, BEREZAN sent a private message through DirectConnection to another co-conspirator titled "offer for you." BEREZAN offered to share the proceeds of fraud committed with stolen payment cards if the co-conspirator loaded

---

[2] A "PIN" is the set of digits (typically four) that must be inputted at the time a debit card is used at an ATM or point-of-sale terminal to request a withdrawal of money from a bank account associated with the debit card.

[3] The term "cashouts" refers to using stolen payment card information to make fraudulent purchases or to withdraw money from bank accounts without authorization.

BEREZAN's "injects for collection of cc, cvv, expiry dates and PINS" into a botnet. BEREZAN added that the scheme would be lucrative given it was "the time now when banks raise limits before new year, so that holders buy expensive gifts :-)."

d. The next year, on or about June 2 and 6, 2011, BEREZAN posted messages within the "Real carding. Documents. Real plastic. Equipment, dumps (cashout/sale). Documents. Scans and documents" forum on DirectConnection requesting assistance in decrypting PINs in a particular format. BEREZAN explained that much of the data was valid and asked to be contacted via private message.

e. The following year, on or about January 4, 2012, BEREZAN posted a message within the "Real carding. Documents. Real plastic. Equipment, dumps (cashout/sale). Documents. Scans and documents" forum on DirectConnection offering assistance in conducting fraud with payment card data (including PINs) in the United States.

f. Similarly, on or about June 7, 2012, BEREZAN posted a message within the "Sale and purchase of cards. Visa, MasterCard, AMEX. COBs, VBV, CVV. Extraction of SSN/DOB and other cardholder information" forum on DirectConnection asking for credit and debit card account numbers and PINs in exchange for 30% to 35% of the proceeds from using those cards to conduct fraudulent transactions. BEREZAN's posting indicated that the fraudulent transactions would take place in the United States.

g. Likewise, on or about April 30, 2015, BEREZAN posted a message within the "Real carding. Documents. Real plastic. Equipment, dumps (cashout/sale). Documents. Scans and documents" forum on DirectConnection requesting assistance "cashing" certain U.S. payment card numbers "with PINs."

h. Then, on July 1, 2015, BEREZAN sent a private message through DirectConnection to another DirectConnection member. The subject line of the message was "Dump + PIN," and the message stated, in relevant part, "[W]e cash out both in US and on POS terminals."

i. And, on or about December 1, 2015, BEREZAN sent a private message to a DirectConnection co-conspirator asking where the user wanted to try cashing out payment card data without PINs, and the co-conspirator responded on or about December 7, 2015, by providing the co-conspirator's contact information for an online instant messaging service known as Jabber.

7. From at least in or around July 2009 and continuing until his apprehension by law enforcement in November 2020, BEREZAN also specialized in providing "drop" services, also referenced herein as "drops." That is, BEREZAN facilitated and managed the movement of fraudulently obtained goods and funds for purposes of circumventing financial institutions' and credit card companies' fraud detection measures and hindering law enforcement's efforts to trace fraudulent transactions. Similar to his efforts to acquire and use stolen payment card data, BEREZAN sought to leverage his DirectConnection membership to form criminal partnerships for purposes of providing drop services. For example:

a. On October 8, 2009, BEREZAN sent a private message through DirectConnection to another DirectConnection co-conspirator that stated BEREZAN had "drops in DE" and provided his contact information for ICQ, which was an instant messaging service. The recipient of this message responded the next day asking if the drops were "duped or non-duped," which, in this context, means whether the individuals receiving and sending the stolen goods or proceeds were doing so knowingly. BEREZAN responded on or about October 12,

2009: "non-duped!" The pair thereafter agreed to use ICQ in order to discuss working together on the drops.

b. Similarly, on or about March 30, 2010, BEREZAN sent a private message through DirectConnection to another DirectConnection user that stated BEREZAN had "drops in [the] US."

c. Likewise, on or about March 25, 2013, a DirectConnection co-conspirator sent a private message to BEREZAN regarding "corporate" and "personal drops" and stated he would give thought to what could be "arranged." BEREZAN responded the same day, providing his Jabber address and asking the DirectConnection co-conspirator to contact him to "talk."

8. BEREZAN also used DirectConnection to facilitate fraud on behalf of others. For example, on or about January 30, 2012, Berezan posted a message within the "Spam. Hosting and traffic. Spam. Downloads and traffic. Hosting, domains and servers" forum on DirectConnection regarding the sale of a database with U.S. data. BEREZAN explained that his acquaintance was willing to sell a database consisting of usernames and passwords for more than "7kk" U.S. users and more than 2 million U.K. users.

9. BEREZAN, in fact, formed a number of criminal partnerships through DirectConnection. Four such partnerships are highlighted below.

BEREZAN and the Drops Co-Conspirator

10. Since at least on or about February 4, 2014, BEREZAN sent private messages through DirectConnection to another DirectConnection co-conspirator interested in drops. The pair agreed on or about July 20, 2015, to traffic stolen goods or proceeds together after having discussed which "non-duped" individuals to hire.

BEREZAN and the Card Source Co-Conspirator

11. Since at least November 2010, BEREZAN communicated with a particular co-conspirator (hereinafter, "Card Source") about stolen payment card data and PINs.

12. For example, on or about November 25, 2010, BEREZAN sent a private message through DirectConnection to Card Source that was titled "hi dump + PIN," stated that BEREZAN could "try to withdraw up to 150k via POS-terminal, 20% are yours," and asked Card Source to contact BEREZAN if he was interested. Card Source responded the next day that he did not "have those for now" but thought he would have stolen payment card data and PINs "in a week" and would "message [BEREZAN] once they're available."

13. Subsequently on or about April 13, 2011, BEREZAN posted a message within the "Sale and purchase of cards. Visa, Mastercard, AMEX. COBs, VBV, CVV. Extraction of SSN/DOB and other cardholder information" forum on DirectConnection. The title of the message was "cc + pin," and BEREZAN later deleted this posting on June 6, 2011.

14. The next day, on or about April 14, 2011, Card Source sent a private message through DirectConnection to BEREZAN regarding BEREZAN's "cc + pin" posting. Card Source provided his Jabber account and stated, in relevant part, "[H]i, I do have that, fresh and on permanent basis. Can I hear more details about the bruteforce? Is it fast/slow, does it kill much, does it only accept debit cards or also credit card, about BoF and so on? Or leave me your Jabber." The exchange of messages referred to BEREZAN'S facilitating the acquisition of stolen payment cards. BEREZAN responded on or about April 18, 2011, writing that he wanted to talk to Card Source via Jabber, and that, "[I]t works with all cards, both credit and debit. [A]s for fast or slow, it depends on quality of the cc. [I]f the cards are fresh, it is fast. [Y]ou set it up today and cream off in the end of the week."

15. By at least June 1, 2011, Card Source agreed to provide BEREZAN with stolen payment card data and did so.

BEREZAN and the Carding Co-Conspirator

16. On or about September 21 and 29, 2010, a DirectConnection member, who will be referred to herein as "Carding Co-Conspirator," sent private messages through DirectConnection to BEREZAN that referenced PINs and provided Carding Co-Conspirator's contact information for ICQ.

17. From at least 2009 and continuing through at least 2012, ICQ had servers located within the Eastern District of Virginia. Messages sent and received through ICQ during this time period, as a result, caused wire communications to be transmitted into and out of servers located in the Eastern District of Virginia.

18. Accordingly, on or about September 29, 2010, and continuing through at least on or about October 9, 2011, BEREZAN's and Carding Co-Conspirator's communications via ICQ caused wire communications to be transmitted between the Eastern District of Virginia and locations outside the Commonwealth of Virginia. Through these communications, BEREZAN and Carding Co-Conspirator agreed to the following arrangement: BEREZAN would send to Carding Co-Conspirator batches of payment card account numbers and related information; Carding Co-Conspirator would process the account information in order to make it useable for fraudulent transactions (referred to as "dumps"); Carding Co-Conspirator would send dumps to BEREZAN, who would then provide the PINs for the dumps; and BEREZAN and Carding Co-Conspirator thereafter would engage in or facilitate cashouts. For instance:

a. On or about November 5, 2010, BEREZAN told Carding Co-Conspirator that he was sending him a batch of payment card account numbers "3.5k" in size, and asked

Carding Co-Conspirator to "process them quickly" because although "the material is fresh . . . many of them are pre-2010 . . . ." Carding Co-Conspirator responded that he would process the information.

b. On or about March 18, 2011, BEREZAN sent messages to Carding Co-Conspirator offering to conduct cashouts on Carding Co-Conspirator's behalf. BEREZAN explained that he could cashout "in the USA" and that his "cashouter takes 19%."

c. On or about March 28, 2011, Carding Co-Conspirator sent BEREZAN 15 payment card account numbers, and BEREZAN responded the same day with the PINs that corresponded to those numbers.

d. On or about May 2, 2011, BEREZAN told Carding Co-Conspirator that he had successfully cashed out about $3,000 from a batch of payment account numbers that the pair had previously shared.

e. On or about May 30, 2011, Carding Co-Conspirator sent BEREZAN 14 payment card account numbers and advised that half of the numbers were for BEREZAN, and sent separately another 23 payment card account numbers and advised that all of these numbers were for BEREZAN. Two days later, on or about June 1, 2011, BEREZAN shared with Carding Co-Conspirator the PINs for each of the 14 account numbers that were to be split between BEREZAN and Carding Co-Conspirator. At least two of the payment card account numbers that Carding Co-Conspirator sent to BEREZAN had been issued by Financial Institution B, a U.S. banking entity headquartered in North Carolina and then insured by the FDIC, including: (i) an account number ending in 7391, which had been issued in the name of an individual residing in New Mexico, and which subsequently was used on or about June 2, 2011, to make $186 in fraudulent purchases at an Apple store located in Brooklyn, New York; and (ii)

an account number ending in 4578, which had been issued in the name of an individual residing in Pennsylvania, and which subsequently was used between on or about June 20 and 23, 2011, to conduct more than $200 in fraudulent transactions at locations in New Jersey and New York.

f. Also, on or about June 1, 2011, BEREZAN and Carding Co-Conspirator exchanged several messages. BEREZAN explained, among other things, that: a dataset containing 1,000 stolen payment cards that BEREZAN previously had provided to Carding Co-Conspirator came from Card Source; that "there won't be any PINs for" Card Source's dataset; and BEREZAN had access to a botnet that was collecting payment account numbers.

g. On or about June 20, 2011, Carding Co-Conspirator sent BEREZAN a message containing 14 payment card account numbers, and BEREZAN responded the same day with the PINs that corresponded to 9 of those account numbers, including an account number ending in 4394 that had been issued by Financial Institution A in the name of an individual residing in Arizona.

h. Also, on or about June 20, 2011, Carding Co-Conspirator, at BEREZAN's request, sent 15 payment card account numbers to BEREZAN via an ICQ instant message. At least one of the account numbers that Carding Co-Conspirator sent to BEREZAN ended in 5127, which was a payment card account number that had been issued by Financial Institution B to an individual residing in Massachusetts, and which subsequently was used between on or about June 22, 2011, and July 12, 2011, to conduct more than $2,200 in fraudulent transactions at locations in the United Kingdom and Estonia.

i. In addition, on or about November 28, 2012, BEREZAN sent a private message to Carding Co-Conspirator through DirectConnection claiming he had approximately 10,000 payment card account numbers to share with Carding Co-Conspirator.

BEREZAN and Co-Conspirator-1

19. BEREZAN began privately messaging Co-Conspirator-1 on DirectConnection as early as on or about June 13, 2012.

20. In or around 2013 and 2014, BEREZAN sent private messages to Co-Conspirator-1 containing BEREZAN's Jabber username and particular email addresses so that they could communicate outside of DirectConnection.

21. Sometime on or before April 17, 2015, a co-conspirator provided BEREZAN with dumps for several payment cards, and BEREZAN sent these dumps to Co-Conspirator-1. On or about April 18, 2015, BEREZAN sent a private message on DirectConnection to Co-Conspirator-1 complaining that Co-Conspirator-1 had not responded yet about the dumps. BEREZAN included in this message dumps for 13 payment cards issued by Financial Institution B and Financial Institution C, a U.S. banking entity headquartered in New York and then insured by the FDIC, including payment account numbers ending in 0532, 2495, 5902, 8509, and 9302 that one or more co-conspirators used between on or about April 17 and 18, 2015, in Miami, Florida, to make fraudulent withdrawals totaling approximately $5,000.

22. On or about April 22, 2015, BEREZAN sent to Co-Conspirator-1 another private message through DirectConnection that, again, complained about Co-Conspirator-1's non-response and stated: "[G]et more responsible. [T]he more material you take, the longer you are gone for."

BEREZAN's Ill-Gotten Gains

23. In addition, up until BEREZAN's arrest in Latvia, BEREZAN engaged in other computer-enabled fraud and intrusions beyond that which are described above with individuals whom he met through DirectConnection.

24. On or about November 3, 2020, Latvian police searched BEREZAN's residence pursuant to a legal assistance request from the United States and found at the location a red Porsche Carrera 911, a black Porsche Cayenne, and a Ducati motorcycle. Authorities also discovered numerous computers and related electronic devices, a Bitcoin storage device, gold jewelry, and €197,980 (Euro) in currency, which was at the time equivalent to approximately $229,656.80 (USD). BEREZAN maintained Bitcoin wallets containing approximately 42.6 Bitcoin. All of this property constituted the proceeds of BEREZAN's participation in the above conspiracies and related criminal conduct.

(CONTINUED ON NEXT PAGE)

25. Based on the above facts, the loss attributable to the 17,542 payment account numbers discussed by BEREZAN with other members of DirectConnection is at least $8,771,000 for Sentencing Guidelines purposes under § 2B1.1, Application Note 3(F)(i).

26. This statement of facts includes those facts necessary to support the plea agreement between the defendant and the United States. It does not include each and every fact known to the defendant or to the United States, and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

27. The actions of the defendant, as recounted above, were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

Respectfully submitted,

Raj Parekh
Acting United States Attorney

Date: April 9, 2021

By: _____

Alexander P. Berrang
Jonathan S. Keim
Assistant United States Attorneys

Laura Fong
Senior Trial Attorney
Computer Crime and Intellectual Property Section
U.S. Department of Justice

Alison Zitron
Trial Attorney
Computer Crime and Intellectual Property Section
U.S. Department of Justice

After consulting with my attorney and receiving explanations and translations in Russian to the extent necessary, pursuant to the Plea Agreement entered into this day, between the defendant, Maksim Berezan, and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

MAKSIM BEREZAN

I am Vadim Glozman, defendant's attorney. I have carefully reviewed the above Statement of Facts with him and explained, to the extent necessary, translated this Statement of Facts into Russian. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Vadim A. Glozman, Esq.
Lana Manitta, Esq.
Counsel for the Defendant